University at Buffalo
The State University of New York

PAYMENT CARD PROCESSING OPTIONS AND PROCEDURES

Payment Card Processing Option	Procedure
In Person – via payment card terminal or SREDKey	• Inform customer of the amount to be charged • Have customer swipe or insert payment card into terminal or SREDKey ○ Do not touch payment card unless required by terminal location • Provide receipt to customer
In Person – no payment card terminal or SREDKey available	• Redirect customer to a UB website for self-entry with customer's own device (e.g., mobile phone, laptop) • If customer self-entry is not an option: ○ Complete the *Payment Card Authorization Form* ○ Have customer sign the *Payment Card Authorization Form* Place *Payment Card Authorization Form* in a lock bag for same-day delivery to the appropriate UB fiscal processing office (hand deliver or use Campus Mail)
Phone – Option 1	• Redirect customer to a UB website for self-entry with customer's own device (e.g., mobile phone, laptop) • If customer self-entry is not an option: ○ Complete the *Payment Card Authorization Form* ○ Confirm amount of the transaction and customer phone number ○ Place *Payment Card Authorization Form* in a lock bag for same-day delivery to the appropriate UB fiscal processing office (hand deliver or use Campus Mail)
Phone – Option 2	• Redirect customer to a UB website for self-entry with customer's own device (e.g., mobile phone, laptop) • If customer self-entry is not an option, direct customer to the appropriate UB fiscal processing office for prompt and secure processing
Mail – payment card transaction received via departmental mail	• Place all information in a lock bag for same day delivery to the appropriate UB fiscal processing office (hand deliver or use Campus Mail)

Payment Card Processing Best Practices

- Do not send payment card information via email
- Do not retain customer information in the department unless these is a specific business purpose
  - If customer information must be retained in the department:
    - Keep only informational data about the transaction and secure in a locked cabinet or drawer
    - Destroy all payment card information using a cross-cut shredder
- Do not save sensitive payment card information electronically (e.g., spreadsheet, UB Box)
- Do not retain the customer payment card
  - If card is left behind or lost, destroy card at the end of the shift, if unable to contact customer
- Do not enter payment card information for customer on a UB computer unless authorized to do so via a SREDKey device
- Do not hold a payment card as a form of collateral